

Administration of Barack H. Obama, 2009

Remarks on Securing the Nation's Information and Communications Infrastructure

May 29, 2009

Hello, everybody. Please be seated. We meet today at a transformational moment, a moment in history when our interconnected world presents us at once with great promise but also great peril.

Now, over the past 4 months, my administration has taken decisive steps to seize the promise and confront these perils. We're working to recover from a global recession while laying a new foundation for lasting prosperity. We're strengthening our Armed Forces as they fight two wars, at the same time we're renewing American leadership to confront unconventional challenges, from nuclear proliferation to terrorism, from climate change to pandemic disease. And we're bringing to Government and to this White House unprecedented transparency and accountability and new ways for Americans to participate in their democracy.

But none of this progress would be possible, and none of these 21st century challenges can be fully met, without America's digital infrastructure, the backbone that underpins a prosperous economy and a strong military and an open and efficient Government. Without that foundation, we can't get the job done.

It's long been said that the revolutions in communications and information technology have given birth to a virtual world. But make no mistake: This world, cyberspace, is a world that we depend on every single day. It's our hardware and our software, our desktops and laptops and cell phones and BlackBerries that have become woven into every aspect of our lives.

It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our Nation. It's the classified military and intelligence networks that keep us safe and the World Wide Web that has made us more interconnected than at any time in human history. So cyberspace is real, and so are the risks that come with it.

It's the great irony of our information age. The very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this paradox, seen and unseen, is something that we experience every day.

It's about the privacy and the economic security of American families. We rely on the Internet to pay our bills, to bank, to shop, to file our taxes. But we've had to learn a whole new vocabulary just to stay ahead of the cyber criminals who would do us harm: spyware and malware and spoofing and phishing and botnets. Millions of Americans have been victimized, their privacy violated, their identities stolen, their lives upended, and their wallets emptied. According to one survey, in the past 2 years alone, cyber crime has cost Americans more than \$8 billion.

I know how it feels to have privacy violated because it has happened to me and the people around me. It's no secret that my Presidential campaign harnessed the Internet and technology to transform our politics. What isn't widely known is that during the general election, hackers managed to penetrate our computer systems. To all of you who donated to our campaign, I

want you to all rest assured, our fundraising web site was untouched. *[Laughter]* So your confidential personal and financial information was protected.

But between August and October, hackers gained access to e-mails and a range of campaign files, from policy position papers to travel plans. And we worked closely with the CIA—with the FBI and the Secret Service and hired security consultants to restore the security of our systems. It was a powerful reminder: In this information age, one of your greatest strengths—in our case, our ability to communicate to a wide range of supporters through the Internet—could also be one of your greatest vulnerabilities.

So this is a matter, as well, of America's economic competitiveness. The small businesswoman in St. Louis, the bond trader in the New York Stock Exchange, the workers at a global shipping company in Memphis, the young entrepreneur in Silicon Valley, they all need the networks to make the next payroll, the next trade, the next delivery, the next great breakthrough. E-commerce alone, last year, accounted for some \$132 billion in retail sales.

But every day we see waves of cyber thieves trolling for sensitive information: the disgruntled employee on the inside, the lone hacker a thousand miles away, organized crime, the industrial spy, and increasingly, foreign intelligence services. In one brazen act last year, thieves used stolen credit card information to steal millions of dollars from 130 ATMs—machines in 49 cities around the world, and they did it in just 30 minutes. A single employee of an American company was convicted of stealing intellectual property reportedly worth \$400 million. It's been estimated that last year alone cyber criminals stole intellectual property from businesses worldwide worth up to \$1 trillion. In short, America's economic prosperity in the 21st century will depend on cybersecurity.

And this is also a matter of public safety and national security. We count on computer networks to deliver our oil and gas, our power and our water. We rely on them for public transportation and air traffic control. Yet we know that cyber intruders have probed our electrical grid and that in other countries cyber attacks have plunged entire cities into darkness.

Our technological advantage is a key to America's military dominance. But our defense and military networks are under constant attack. Al Qaida and other terrorist groups have spoken of their desire to unleash a cyber attack on our country, attacks that are harder to detect and harder to defend against. Indeed, in today's world, acts of terror could come not only from a few extremists in suicide vests, but from a few key strokes on the computer, a weapon of mass disruption.

In one of the most serious cyber incidents to date against our military networks, several thousand computers were infected last year by malicious software, malware. And while no sensitive information was compromised, our troops and defense personnel had to give up those external memory devices, thumb drives, changing the way they used their computers every day.

And last year, we had a glimpse of the future face of war. As Russian tanks rolled into Georgia, cyber attacks crippled Georgian Government web sites. The terrorists that sowed so much death and destruction in Mumbai relied not only on guns and grenades but also on GPS and phones using voice-over-the-Internet. For all these reasons, it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation.

It's also clear that we're not as prepared as we should be, as a Government or as a country. In recent years, some progress has been made at the Federal level. But just as we failed in the past to invest in our physical infrastructure—our roads, our bridges, and rails—we've failed to invest in the security of our digital infrastructure.

No single official oversees cybersecurity policy across the Federal Government, and no single agency has the responsibility or authority to match the scope and scale of the challenge. Indeed, when it comes to cybersecurity, Federal agencies have overlapping missions and don't coordinate and communicate nearly as well as they should, with each other or with the private sector. We saw this in the disorganized response to Conficker, the Internet worm that in recent months has infected millions of computers around the world.

This status quo is no longer acceptable, not when there's so much at stake. We can and we must do better. And that's why shortly after taking office I directed my National Security Council and Homeland Security Council to conduct a top-to-bottom review of the Federal Government's efforts to defend our information and communications infrastructure and to recommend the best way to ensure that these networks are able to secure our networks as well as our prosperity.

And our view—our review was open and transparent. I want to acknowledge, Melissa Hathaway, who is here, who is the Acting Senior Director for Cyberspace on our National Security Council, who led the review team, as well as the Center for Strategic and International Studies bipartisan Commission on Cybersecurity, and all who were part of our 60-day review team. They listened to a wide variety of groups, many of which are represented here today and I want to thank for their input: industry and academia, civil liberties and private—privacy advocates. We listened to every level and branch of Government, from local to State to Federal, civilian, military, homeland as well as intelligence, Congress, and international partners as well. I consulted with my national security teams, my homeland security teams, and my economic advisers.

Today I'm releasing a report on our review and can announce that my administration will pursue a new comprehensive approach to securing America's digital infrastructure. This new approach starts at the top with this commitment from me: From now on, our digital infrastructure, the networks and computers we depend on every day, will be treated as they should be, as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy, and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage.

To give these efforts the high-level focus and attention they deserve—and as part of the new, single national security staff announced this week—I'm creating a new office here at the White House that will be led by the cybersecurity coordinator. Because of the critical importance of this work, I will personally select this official. I'll depend on this official in all matters relating to cybersecurity, and this official will have my full support and regular access to me as we confront these challenges.

Today I want to focus on the important responsibilities this office will fulfill: orchestrating and integrating all cybersecurity policies for the Government, working closely with the Office of Management and Budget to ensure agency budgets reflect those priorities, and in the event of major cyber incident or attack, coordinating our response.

To ensure that Federal cyber policies enhance our security and our prosperity, my cybersecurity coordinator will be a member of the national security staff, as well as the staff of my National Economic Council. To ensure that policies keep faith with our fundamental values, this office will also include an official with a portfolio specifically dedicated to safeguarding the privacy and civil liberties of the American people.

There's much work to be done, and the report we're releasing today outlines a range of actions that we will pursue in five key areas.

First, working in partnership with the communities represented here today, we will develop a new comprehensive strategy to secure America's information and communications networks. To ensure a coordinated approach across Government, my cybersecurity coordinator will work closely with my Chief Technology Officer, Aneesh Chopra, and my Chief Information Officer, Vivek Kundra. To ensure accountability in Federal agencies, cybersecurity will be designated as one of my key management priorities. Clear milestones and performance metrics will measure progress. And as we develop our strategy, we will be open and transparent, which is why you'll find today's report and a wealth of related information on our web site, www.whitehouse.gov.

Second, we will work with all the key players, including State and local governments and the private sector, to ensure an organized and unified response to future cyber incidents. Given the enormous damage that can be caused by even a single cyber attack, ad hoc responses will not do, nor is it sufficient to simply strengthen our defenses after incidents or attacks occur. Just as we do for natural disasters, we have to have plans and resources in place beforehand, sharing information, issuing warnings, and ensuring a coordinated response.

Third, we will strengthen the public/private partnerships that are critical to this endeavor. The vast majority of our critical information infrastructure in the United States is owned and operated by the private sector. So let me be very clear: My administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity.

Fourth, we will continue to invest in the cutting-edge research and development necessary for the innovation and discovery we need to meet the digital challenges of our time. And that's why my administration is making major investments in our information infrastructure: laying broadband lines to every corner of America, building a smart electric grid to deliver energy more efficiently, pursuing a next generation of air traffic control systems, and moving to electronic health records, with privacy protections, to reduce costs and save lives.

And finally, we will begin a national campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms and to build a digital workforce for the 21st century. And that's why we're making a new commitment to education in math and science and historic investments in science and research and development. Because it's not enough for our children and students to master today's technologies—social networking and e-mailing and texting and blogging—we need them to pioneer the technologies that will allow us to work effectively through these new media and allow us to prosper in the future. So these are the things we will do.

Let me also be clear about what we will not do. Our pursuit of cybersecurity will not include—I repeat, will not include—monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans. Indeed, I remain firmly committed to net neutrality so we can keep the Internet as it should be, open and free.

The task I have described will not be easy. Some 1.5 billion people around the world are already online, and more are logging on every day. Groups and governments are sharpening their cyber capabilities. Protecting our prosperity and security in this globalized world is going to be a long, difficult struggle demanding patience and persistence over many years.

But we need to remember we're only at the beginning. The epochs of history are long: the agricultural revolution, the Industrial Revolution. By comparison, our information age is still in its infancy. We're only at Web 2.0. Now our virtual world is going viral, and we've only just begun to explore the next generation of technologies that will transform our lives in ways we can't even begin to imagine.

So a new world awaits, a world of greater security and greater potential prosperity, if we reach for it, if we lead. So long as I'm President of the United States, we will do just that. And the United States, the Nation that invented the Internet, that launched an information revolution, that transformed the world, will do what we did in the 20th century and lead once more in the 21st.

Thank you very much, everybody. Thank you.

NOTE: The President spoke at 11:08 a.m. in the East Room at the White House.

Categories: Addresses and Remarks : Securing information and communications infrastructure.

Locations: Washington, DC.

Names: Chopra, Aneesh; Hathaway, Melissa; Kundra, Vivek.

Subjects: Arms and munitions : Nuclear weapons and material :: Nonproliferation efforts; Business and industry : Internet commerce; Commerce, international : Global financial markets :: Unrest; Defense and national security : Cyber attacks; Defense and national security : Cybersecurity, strengthening efforts; Diseases : Global influenza outbreak; Economic Council, National; Economy, national : Strengthening efforts; Education : Science and math programs; Energy : Infrastructure and grid improvements; Environment : Climate change; Georgia, Republic of : Conflict with Russia; Government organization and employees : Accountability and transparency, strengthening efforts; Health and medical care : Information technology; India : Terrorist attacks in Mumbai; Law enforcement and crime : Identity theft; Russia : Conflict with Georgia; Science and technology : Broadband technology; Science and technology : Research and development; Security Council, National; Terrorism : Al Qaida terrorist group; Terrorism : Global threat; White House Office : Assistants to the President :: Chief Technology Officer; White House Office : Assistants to the President :: Chief Information Officer.

DCPD Number: DCPD200900410.